# UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF FLORIDA

UNITED STATES OF AMERICA,

Plaintiff,

v.

FLUENT, LLC;

REWARDZONE USA LLC, also d/b/a Up Rewards, The Reward Genius, Flash Rewards, and National Consumer Center;

DELIVER TECHNOLOGY LLC, also d/b/a Flash Rewards;

SEARCH WORKS MEDIA, LLC, also d/b/a FindDreamJobs and StartACareerToday; and

EASE WINS, LLC, also d/b/a JobsOnDemand; Defendants.

Case No. 9:23-cv-81045

COMPLAINT FOR CIVIL PENALTIES, PERMANENT INJUNCTION, MONETARY RELIEF, AND OTHER RELIEF

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC"), pursuant to Section 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 56(a)(1), for its Complaint alleges:

1. Plaintiff brings this action under Sections 5(a), 5(m)(1)(A), 13(b), 16(a), and 19 of the FTC Act, 15 U.S.C. §§ 45(a), 45(m)(1)(A), 53(b), 56(a), and 57b, Section 6 of the Telemarketing and Consumer Fraud and Abuse Prevention Act (the "Telemarketing Act"), 15 U.S.C. § 6105, and Section 7(a) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C. § 7706(a), to obtain monetary civil penalties, a permanent injunction, and other equitable relief for Defendants' violations of Section

- 5(a) of the FTC Act, 15 U.S.C. § 45(a), the FTC's Telemarketing Sales Rule (the "TSR"), as amended, 16 C.F.R. Part 310, and the CAN-SPAM Act, 15 U.S.C. §§ 7701–7713.
- 2. Defendants have operated a massive "consent farm" enterprise, using deceptive ads and websites to induce nearly one million consumers a day to provide their personal information and purported consent to receive telemarketing calls. In turn, Defendants have aggregated consumers' personal information and sold it to numerous telemarketers, who have relied on consumers' purported consent to justify robocalls and calls to numbers on the National Do-Not-Call Registry. All told, Defendants have sold the information of millions of consumers, generating tens of millions of dollars in revenue.
- 3. Defendants' "consent farm" business is unlawful. To induce consumers to provide their personal information, Defendants and their affiliate marketers have misleadingly promised consumers job interviews and free rewards, when in fact the promised jobs typically did not exist, and the promised rewards were virtually impossible to obtain. Moreover, Defendants have failed to clearly disclose to consumers that the true purpose for collecting their personal information was for telemarketing, not job and reward offers. Finally, the purported consent that Defendants has obtained from consumers has been insufficient under the TSR. Thus, Plaintiff files this suit to recover civil penalties and halt Defendant's unlawful conduct.

## JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), 1345, and 1355, because it involves claims arising under federal laws regulating commerce and is commenced by the United States. The claims arise under 15 U.S.C. §§ 45(m)(1)(A), 53(b), and 56(a).

5. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) and 15 U.S.C. § 53(b), because Defendants transact business in this District, and a substantial part of the events or omissions giving rise to the claims occurred in this District.

# **DEFENDANTS**

- 6. Defendant Fluent, LLC is a Delaware limited liability company with its principal place of business at 300 Vesey Street, 9th Floor, New York, NY 10282. Fluent, LLC transacts or has transacted business in this District and throughout the United States. Fluent, LLC wholly owns Defendants RewardZone USA LLC, Deliver Technology LLC, Search Works Media, LLC, and Ease Wins, LLC. At all times relevant to this Complaint, acting alone or in concert with others, Fluent, LLC has acquired information from consumers throughout the United States and then advertised, marketed, distributed, or sold that information as leads to third parties throughout the United States.
- 7. Defendant RewardZone USA LLC ("RewardZone"), also doing business as Level Up Rewards, The Reward Genius, Flash Rewards, and National Consumer Center, is a Delaware limited liability company with its principal place of business at 300 Vesey Street, 9th Floor, New York, NY 10282. RewardZone transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, RewardZone has acquired information from consumers throughout the United States and then advertised, marketed, distributed, or sold that information as leads to third parties throughout the United States.
- 8. Defendant Deliver Technology LLC, also doing business as Flash Rewards, is a Delaware limited liability company with its principal place of business at 300 Vesey Street, 9th Floor, New York, NY 10282. Deliver Technology transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or

in concert with others, Deliver Technology has acquired information from consumers throughout the United States and then advertised, marketed, distributed, or sold that information as leads to third parties throughout the United States.

- 9. Defendant Search Works Media, LLC, also doing business as FindDreamJobs and StartACareerToday, is a Delaware limited liability company with its principal place of business at 300 Vesey Street, 9th Floor, New York, NY 10282. Search Works Media transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Search Works Media has acquired information from consumers throughout the United States and then advertised, marketed, distributed, or sold that information as leads to third parties throughout the United States.
- 10. Defendant Ease Wins, LLC, also doing business as JobsOnDemand, is a Delaware limited liability company with its principal place of business at 300 Vesey Street, 9th Floor, New York, NY 10282. Ease Wins transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Ease Wins has acquired information from consumers throughout the United States and then advertised, marketed, distributed, or sold that information as leads to third parties throughout the United States.

#### **COMMON ENTERPRISE**

11. Defendants Fluent, RewardZone, Deliver Technology, Search Works Media, and Ease Wins (collectively, "Defendants" or "Fluent") have operated as a common enterprise while engaging in the unlawful practices alleged below. Defendants have conducted the business practices described below through an interrelated network of companies that have common ownership, business functions, employees, and office locations. Because Defendants have operated as a common enterprise, each of them is liable for the acts and practices alleged below.

## **COMMERCE**

12. At all times relevant to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

# THE FEDERAL TRADE COMMISSION ACT

- 13. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."
- 14. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

# THE TELEMARKETING SALES RULE

- 15. Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101, 6108. The FTC adopted the original TSR in 1995, extensively amended it in 2003, and amended certain provisions thereafter. 16 C.F.R. Part 310.
- 16. Under the TSR, an "outbound telephone call" means a telephone call initiated by a telemarketer to induce the purchase of goods or services or to solicit a charitable contribution. *Id.* § 310.2(x). A "seller" means any person who, in connection with a telemarketing transaction, provides, offers to provide, or arranges for others to provide goods or services to the customer in exchange for consideration. *Id.* § 310.2(dd). A "telemarketer" means any person who, in connection with telemarketing, initiates or receives telephone calls to or from a customer or donor. *Id.* § 310.2(ff).
- 17. As amended, effective September 1, 2009, the TSR prohibits initiating any outbound telephone call that delivers a prerecorded message (a "robocall") to induce the purchase of any good or service, unless the seller has obtained from the recipient of the call an express

agreement, in writing, that evidences the willingness of the recipient of the call to receive calls that deliver prerecorded messages by or on behalf of a specific seller.  $Id. \S 310.4(b)(l)(v)$ . The express agreement the seller has obtained from the recipient of the call must include: (i) A clear and conspicuous disclosure that the purpose of the agreement is to authorize the seller to place prerecorded calls to such person; (ii) Evidence that the seller obtained without requiring, directly or indirectly, that the agreement be executed as a condition of purchasing any good or service; (iii) Evidence of the willingness of the recipient of the call to receive calls that deliver prerecorded messages by or on behalf of a specific seller; and (iv) The recipient's telephone number and signature.  $Id. \S 310.4(b)(l)(v)(A)$ . Under the TSR, the express agreement may not be obtained by a lead generator who does not qualify as a seller or telemarketer under the TSR because the express agreement must be obtained by the seller or telemarketer directly from the call recipient.

- 18. Additionally, the 2003 amendments to the TSR established the National Do-Not-Call Registry ("Registry"), maintained by the FTC, of consumers who do not wish to receive certain types of telemarketing calls. Consumers can register their telephone numbers on the Registry without charge either through a toll-free telephone call or over the Internet at donotcall.gov.
- 19. The TSR prohibits sellers and telemarketers from initiating an outbound telephone call to a number on the Registry unless the seller or telemarketer can demonstrate that the seller (1) has obtained the consumer's express agreement, in writing, to place such calls, or (2) has an established business relationship with that consumer, and the consumer has not stated that he or she does not wish to receive such calls. *Id.* § 310.4(b)(l)(iii)(B). Valid written consent to receive a live telemarketing call to a number on the Registry requires: (1) a writing signed by the consumer,

- (2) clearly evidencing authorization to receive calls placed by or on behalf of a specific party, and (3) stating the telephone number to which such calls may be placed. *Id.* § 310.4(b)(l)(iii)(B)(l).
- 20. Consumers who receive telemarketing calls to their registered numbers can complain of Registry violations the same way they registered, through a toll-free telephone call or over the Internet at *donotcall.gov*, or by otherwise contacting law enforcement authorities.
- 21. The FTC allows sellers, telemarketers, and other permitted organizations to access the Registry over the Internet at *telemarketing.donotcall.gov*, to pay the fee(s) if required, and to download the numbers not to call.
- 22. Certain sections of the TSR apply to individuals or companies other than "sellers" or "telemarketers" if these individuals or companies provide substantial assistance or support to sellers or telemarketers. Pertinent here, it is a violation of the TSR for any person to provide substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any practice that violates Sections 310.3(a), (c) or (d), or 310.4 of the TSR. *Id.* § 310.3(b).
- 23. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c), a violation of the TSR is treated as a violation of an FTC rule under Section 18 of the FTC Act, 15 U.S.C. § 57a, regarding unfair or deceptive acts or practices. In turn, under Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

#### THE CAN-SPAM ACT

24. Section 5(a)(1) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(1), states: "It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message [an "email"] . . . that contains, or is accompanied by, header information that is materially false or misleading."

- 25. Under the CAN-SPAM Act, "header information" is defined as "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." 15 U.S.C. § 7702(8).
- 26. Section 6(a) of the CAN-SPAM Act, 15 U.S.C. § 7705(a), further deems it is unlawful "to promote, or allow the promotion, of [the] person's trade or business, or goods, products, property, or services" that the person makes available, through an email whose transmission violates Section 5(a)(1), if that person: (1) knew or should have known about the promotion; (2) received or expected to receive an economic benefit from the promotion; and (3) failed to take reasonable action to prevent the transmission or to detect and report the transmission to the FTC.
- 27. Section 5(a)(2) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(2), also declares it unlawful "to initiate the transmission to a protected computer of a commercial [email] if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the content or subject matter of the message," consistent with the criteria used to enforce Section 5 of the FTC Act.
- 28. Section 7(e) of the CAN-SPAM Act, 15 U.S.C. § 7706(e), states that in any action to enforce compliance through an injunction with Section 5(a)(2) and other specified sections of the CAN-SPAM Act, the Government need not allege or prove the state of mind required by such sections.

- 29. Lastly, Section 5(a)(4) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(4), renders it unlawful to initiate the transmission of a commercial email to a recipient from whom it received, more than ten days before, a request not to receive commercial emails from the sender.
- 30. Pursuant to Section 7(c) of the CAN-SPAM Act, 15 U.S.C. § 7706(c), a violation of the CAN-SPAM Act is treated as a violation of an FTC rule under Section 18 of the FTC Act, 15 U.S.C. § 57a, regarding unfair or deceptive acts or practices. In turn, under Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the CAN-SPAM Act constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

## **DEFENDANTS' UNLAWFUL CONDUCT**

- 31. Since at least 2011, Defendants have operated a massive online lead generation enterprise that has deceptively induced tens of millions of consumers to disclose their personal information. Defendants have aggregated and sold consumers' information to their clients, who have used that information to inundate consumers with telephone, text message, and email solicitations about a multitude of products and services, including pain cream, for-profit education, insurance products, solar energy, extended auto warranties, debt reduction, medical alert devices, and more.
- 32. To obtain consumers' personal information, Defendants have relied on thousands of lead generation websites. Defendants have claimed to regularly receive over 900,000 registrations per day on their lead generation websites. Moreover, from January 2018 to December 2019, Defendants sold over 620 million leads, generating \$93.4 million in revenue.
- 33. Defendants have funneled consumers to their websites by disseminating their own ads, and by paying affiliate marketers (or "publishers") to disseminate ads containing hyperlinks to the Fluent lead generation sites. Defendants know or should know that their publishers often use

ads that are facially deceptive, and make use of other abusive tactics, such as text message spamming and browser hijacking. Nevertheless, Defendants have failed to prevent their publishers from engaging in this illicit conduct. In fact, Fluent sales executives have excused and even encouraged this conduct.

- 34. Moreover, many of Defendants' ads have made unauthorized use of the trademarks of well-known brands as a way of misleading consumers into believing that Defendants are affiliated with or endorsed by these brands. For example, Defendants' ads often feature the trademarked logos of Amazon and Cash App, a peer-to-peer money transfer service owned by Block, Inc. In takedown letters, suspension requests to a domain registrar, and an intellectual property complaint, Amazon and Block have repeatedly warned Defendants that their ads infringe these companies' trademarks, deceive consumers regarding Defendants' affiliation with their brands, and appear to be part of scam to deceive consumers into disclosing their personal information. Despite these warnings, Defendants have continued to feature the infringing trademarks in their ads.
- 35. After receiving a Civil Investigative Demand at the outset of the FTC's investigation in early 2020, Defendants announced new measures purportedly designed to rein in their publishers. As a part of this alleged "compliance initiative," Defendants began relying less on publishers and more on their own advertising as a way of drawing consumers to their lead generation websites. Defendants' compliance initiative has been an abject failure. Fluent publishers have continued to distribute brazenly deceptive ads that Defendants could quickly and easily find and stop if they wanted to do so. Moreover, Defendants' own ads are misleading.
- 36. Defendants' lead generation websites reinforce and expand on the misleading claims used in the ads. Among other things, the websites use deceptive design techniques,

commonly known as "dark patterns," as well as other tricks, to manipulate consumers into divulging their contact information to Defendants, who sell this information to hundreds of so-called "marketing partners." Defendants conceal names of these entities from consumers in barely legible print behind a hyperlink.

- 37. Defendants' have operated at least two different types of misleading websites. First, Defendants' "reward sites" offer or promise consumers valuable items such as smart phones, cash awards, and gift cards that are redeemable at well-known retailers such as Walmart and Amazon. Defendants' and their publishers' ads claim that these rewards are "free" or can be obtained through a "fast and easy" process that is capable of being completed in a matter of minutes or days, and at no cost. These claims are false. In reality, earning a reward is an onerous, costly, time-consuming, and confusing ordeal that less than 1% of consumers successfully complete.
- 38. Second, Defendants' "job sites" purportedly enable consumers to find employment opportunities. While Defendants' job sites are designed to look like conventional employment search websites, they in fact require consumers to enter a variety of personal information, such as their names, addresses, and dates of birth, before displaying results. Defendants' and their publishers' job ads promise consumers that they can earn lucrative wages and generous benefits, but the promised jobs often do not exist.

## I. Publishers' False and Misleading Ads

39. Defendants have recruited and paid publishers to attract consumers to their lead generation websites. Publishers drive traffic to these sites by circulating ads via different media channels, including email, push notifications, text messages, banner ads, and posts on social media platforms such as Facebook, Instagram, and TikTok.

- 40. In some cases, publishers' ads link directly to Defendants' websites. In others, the ads first link to an intermediary website, known as a "pre-lander," that may display additional claims or attempt to collect information before directing consumers to Defendants' websites.
- 41. To drive traffic to Defendant's websites, Defendants have also allowed publishers to employ their own networks of publishers with whom Defendants have no contractual relationship and about whom Defendants generally know nothing.

## A. Publishers' Deceptive Reward Ads

42. As set forth below, Fluent's publishers have used a variety of tactics to deceive consumers into clicking on their reward ads, including: (a) falsely claiming that the consumer viewing the ad has won or been specially selected to receive a promised reward; (b) gaining consumers' trust by falsely purporting to be affiliated with well-known brands and retailers such as Amazon, Google, Walmart, Verizon, and YouTube; (c) deceptively claiming that consumers will receive a reward in exchange for completing a survey; and (d) pressuring consumers into believing that they must act quickly because only a limited number of rewards are available.

## i. Deceptive Emails

- 43. Defendants' publishers have disseminated emails promoting Defendants' reward sites. These emails have contained materially false or misleading "from" and "subject" lines in order to encourage consumers to open the messages. Examples include:
- a. Using "from" lines such as "Paypal" and "McDonalds," suggesting an affiliation with these brands, or "Congratulations," suggesting that a consumer has won something; and
- b. Using subject headings such as "Confirmed: Your Thousand Dollar Wells Fargo Offer" and "[NAME] Please Accept Your \$750 CashApp Funds or Surrender It!" Again, these headings suggest that the consumer won something.

- 44. The publisher emails also contained deceptive messages promising that consumers will receive a free gift card or other reward. For example:
- a. "Thank you for your order! As a valued shopper, you are now eligible to earn a \$1,000 Amazon gift card\* for responding to a 3 question survey to improve online customer experience." Compl. Attach. 1, at 1; and
- b. "RE: Your CASH APP Deposit (\$750) . . . An unclaimed balance of \$750 is now available for direct deposit to your CASH APP account." Compl. Attach. 1, at 2.
- 45. Consumers who click on buttons or links in these emails are directed to Defendants' lead generation websites.

# ii. Deceptive Text Messages

- 46. Defendants' publishers have disseminated text messages that falsely promising recipients that they have won a gift card or other reward. These messages misleadingly suggest that they originate from the brand associated with the reward. Examples of these misleading text messages include:
- a. "Congrats! Your unique code 5FR-B4X2 printed on your last Walmart receipt is among 7 codes we randomly picked for \$1000 gift card giveaway!"
- b. "Hey, It's Walmart's 60th birthday. We are rewarding 100 lucky loyal customers with a \$1000 gift cards [sic] every day! Claim yours now > [link]."
  - c. "750USD Cash\*App requires your confirmation [link]"
  - d. "Your \$1000 Walmart Giftcard is reserved for 4:51 minutes."
- 47. Again, clicking on the link in one of these text messages directs consumers to Defendants' lead generation websites.

# iii. Deceptive Pop-Up Ads

- 48. Defendants' publishers have also promoted Defendants' reward sites using false and misleading pop-up ads that appear on mobile and desktop web browsers.
- 49. In numerous instances, consumers who encounter these ads are unable to close the ad windows and are forcibly redirected to other websites. This practice, commonly known as browser hijacking, is the source of a constant stream of consumer complaints to Defendants as well as frequent internal discussions, with one Fluent sales executive describing the problem as a "never ending circle."
- 50. These pop-ups often misleadingly claim to originate from well-known companies such as Verizon, Amazon, and Walmart. They also falsely claim that consumers were specially selected to receive a free gift card. *See* Compl. Attach. 1, at 3-5.
- 51. Consumers who click on buttons or links in these ads are directed to Defendants' websites.

#### iv. Deceptive Social Media Ads

- 52. Publishers have also promoted Fluent's reward websites through false and misleading content posted on social media platforms, including TikTok and Instagram, claiming that consumers can obtain a free reward.
- 53. As an example, one of Defendants' publishers maintains a TikTok account, "cashapp935" with over 18,000 followers. The account profile states: "Hurry up everyone!! Claim link below and follow step by step you will get \$250" followed by a hyperlink. Following the account hyperlink leads to a pre-lander website labeled the "CASHAPP Money Generator," which prompts visitors to input their CashApp username and click a "CONTINUE" button.
- 54. Visitors are then taken to a third screen on the pre-lander website where they are instructed to "complete any offers below to verify your account." These offers include, "Your

chance to get \$750 to your Cash App account." If a consumer selects this option, they are directed to one of Fluent's reward websites.

- 55. As another example, one of Defendants' publishers maintains an Instagram account "topfreegiftcards." This account, with over 1,100 followers, has posted an image of what appears to be a \$100 Amazon gift card along with several hashtags, including #amazongiftcardfree, #amazongiftcardgiveaways, #freegiftcard, and #freegiftcardgiveaway.
- 56. Following a link in the account bio leads to a pre-lander website, where can "Claim your FREE GIFT CARD." Clicking an Amazon gift card image opens a new page with the heading, "Want some FREE AMAZON GIFT CARD," along with the instruction to "choose your card amount" between \$25 and \$100. There is also a warning that there are "Only 194 AMAZON CARDS left!"
- 57. Selecting one of the gift card amounts opens a pop-up with the heading "FREE GIFT CARDS" and the instruction to choose one of five rewards, including a \$1,000 Visa gift card. Selecting this option directs to one of the Fluent lead generation websites.

# B. <u>Publishers' Deceptive Job Ads</u>

- 58. Defendants' publishers have also used misleading tactics in order to deceive consumers into clicking on job ads. Among other things, publishers have falsely claimed that consumers were pre-screened on behalf of prospective employers, including well-known companies such as UPS and FedEx. Publishers' job-related emails have also falsely claimed either that a specific employer has scheduled an interview with the recipient or offered to conduct an interview.
- 59. Examples of false or misleading message content in job-related emails promoting Fluent's sites include:

- a. "This is our 3<sup>rd</sup> attempt to reach you at [email]... You can verify an appointment for the job you like by hurrying over to the following website. Wal\*Mart INTERVIEW ASAP [hyperlink]"; and
- b. An email with the subject "RE: Your upcoming interview" along with the messages "UPS is Hiring! \$22/Hr + Up."
- 60. Defendants have received hundreds of complaints and inquiries from consumers about these deceptive emails. As illustrated by the following complaints and inquiries, consumers looking for employment are convinced by the emails that they have been selected for an interview with a prospective employer:
- a. "Why do I keep getting: this is your 2<sup>nd</sup> notice this is your 3<sup>rd</sup> notice for interviews and when I click on it it just gives me more jobs??? If you don't have [an] interview set up, stop saying you do. This is so MISLEADING!";
- b. "I can never get [an] answer to my interview with Amazon...could you please let me know when and do I have my interview"; and
- c. "You telling [me] I got job interviews but I can't never find them to verify them what is going on I really need a job [and] feel like you are just pulling my leg [and] it is not funny to someone like me who wants to work."

## II. Defendants Know of, Authorize, and Further Their Publishers' Misconduct

- 61. Defendants' publishers are supposed to be subject to Defendants' oversight.

  Defendants have required each publisher to execute a contract captioned "Terms and Conditions to Publisher Insertion Orders." This contract, along with compliance guidelines, sets the terms of Defendants' business relationship with their publishers.
- 62. Under the contract, publishers are required to promote Defendants' lead generation websites using marketing materials (or "creatives") provided by Defendants. They have no

authority under the contract to "edit or otherwise modify the Creative or any component therefore" without obtaining "prior written consent" from Defendants. Moreover, any modifications to creatives must comply with Defendants' "marketing restrictions and creative guidelines."

- 63. Defendants maintain multiple sets of creative and advertising guidelines that publishers are required to follow. Among other things, these guidelines prohibit the use of words like "win," "won," or "congratulations" in ads because they suggest that rewards can be obtained without cost to consumers. Defendants have regularly failed to enforce these guidelines, however, even when they know that publishers are flagrantly and repeatedly violating the guidelines.
- 64. Under the publisher contracts, Defendants are supposed to actively monitor publishers and take remedial actions when a publisher violates the creatives guidelines. Until around February 2021, Defendants' compliance policy regarding publisher discipline consisted of the following two-tiered system:
- a. For behavior subject to simple remedial or corrective actions such as minor violations involving the single use of unapproved language, Defendants' policy calls for sending notice of the violation to the publisher and requiring correction of the issue; or
- b. For material non-compliant behavior such as the use of deceptive email headers or repeat use of unapproved language, Defendants' policy considers this beyond any corrective measure, so termination of the relationship is required.
- 65. In communications with regulators and other third parties, Defendants have claimed to aggressively police compliance with their creative guidelines and publisher contracts. For example, in connection a June 2017 application for accreditation with the Better Business Bureau, Fluent's compliance director made the following claim: "We carefully review all

advertisements promoting the Fluent Websites [sic] and our agreements with our publishers. We prohibit them from modifying or revising our advertisements without prior approval."

- 66. In fact, despite the existence of their compliance policy and the authority available to Defendants under their contracts to discipline and terminate non-compliant publishers, Defendants have tacitly or explicitly approved publisher misconduct and ignored clear evidence of unlawful practices, including repeated warnings from an outside compliance monitoring service.
- 67. Defendants typically allow sales executives, who are responsible for sustaining and growing revenue, to oversee compliance matters related to the publishers they manage. This oversight generally occurs on an ad hoc basis, often without the involvement of compliance staff, and rarely results in the termination of a publisher regardless of the number and severity of violations. As a result, Defendants have allowed and encouraged publishers to continue promoting Defendants' websites even in the face of substantial evidence of misconduct.
- 68. Defendants' compliance problems are exemplified by a presentation circulated to Fluent staff in August 2018 addressing the Fluent creative guidelines. This presentation, created by a legal intern and reviewed by the company's general counsel, effectively acknowledges the deceptive conduct regularly engaged in by publishers to promote Defendants' websites and excuses this misconduct. It does so by articulating a "general principle of advertising law" identified as "Funnel Theory." According to the presentation, this theory stands for the proposition that disclosures must be "more comprehensive and clearer" as consumers move closer to the point of purchase. For this reason, the presentation asserts, banner ads and emails "can be more aggressive and ambiguous than a landing page." Legally, this is not correct.

69. As a factual matter, moreover, as described above, Defendants' disclosures on their own websites as consumers move closer to the point of attempting to obtain the offered reward or employment opportunity are not clear and conspicuous and do not clear up the previous deception.

## A. Defendants Fail to Stop Publishers' Misconduct

- 70. Defendants are aware of their publishers' widespread use of facially deceptive, materially non-compliant ads, yet they have failed to put an end to their deception.
- 71. From 2014 through 2021, Defendants subscribed to a compliance monitoring service known as Lashback that generated an alert when it detected that a publisher email did not comply with Fluent's creative guidelines. These alerts typically consisted of a copy of the email, including the header, subject line, and any creatives in the body of the message, as well as information allowing Defendants to identify the responsible publisher. Lashback regularly alerted Defendants about publisher emails falsely claiming that consumers had been specially selected to receive a reward through the use of terms such as "win," "won," "winner," "gift," and "congratulations" and that fail to note that obtaining a reward requires paid participation. From July 2019 to February 2021, LashBack flagged thousands of publisher emails promoting Fluent sites with deceptive "from" and subject lines as well as deceptive message content.
- 72. Despite this evidence, Defendants have typically failed to discipline or terminate non-compliant publishers because the authority to do so rests with Fluent sales executives, who often undercut, ignore, or circumvent compliance processes.
- 73. A particularly egregious case concerns a publisher known as Sphere Digital. Between September 2018 and January 2020, Lashback generated dozens of alerts about deceptive Sphere emails that violated Fluent's creative guidelines. These violations included:
  - a. "CONGRATS You've received \$100 McDonalds Gift Card"

- b. "PayPal Reward Open Immediately...Please Confirm Your \$1,000 PayPal Gift Card. Click HERE"; and
  - c. "CONGRATS You've received \$1,000 VISA Gift Card."
- 74. Sphere's persistent use of deceptive ads was a source of concern at Fluent as far back as July 2018, when Defendants' compliance manager informed the sales team that, despite repeated warnings, Sphere Digital and its affiliates continued to disseminate emails falsely informing consumers that they had "won" rewards. The compliance manager requested that Sphere be "read the riot act" by the sales team and stated that Sphere was just a single "violation away from removal from [the] Fluent network."
- 75. Despite these concerns, Fluent's publisher development manager continued excusing blatant misconduct by Sphere. For example, in November 2018, she informed Sphere about a deceptive Walmart gift card email sent by one of its affiliates. When Sphere offered to terminate the affiliate, the Fluent manager declined the offer, explaining: "Hey, we don't need to pull them. We just need to add [a paid participation disclosure]. This is not a big deal or a huge violation but they need to do it." This same manager had previously advised Sphere to be "as aggressive as possible" with its email subject lines "to maximize opens and clicks" and offered the following, facially deceptive suggestion: "I find anything with congratulations works well."
- 76. A strikingly similar incident involving a different publisher, Maxbounty, took place in June 2019. The same sales manager forwarded a Lashback alert to Maxbounty relating to a deceptive email sent by a Maxbounty affiliate. In response, Maxbounty offered to tell the affiliate not to send unapproved emails, but jokingly noted that "affiliates like to ignore instructions [smiley face emoji]." The manager responded: "Totally fine…this is why we don't work with affiliates direct! LOL [smiley face emoji]."

- 77. Fluent sales executives have openly acknowledged that compliance is secondary to revenue. For example, the sales team intervened on behalf of one publisher, Nexys Media Inc. after it was the subject of an October 2018 consumer complaint with the New York Office of the Attorney General as well as multiple subsequent Lashback alerts showing clear, material violations of Fluent's creative guidelines. In April 2019, Fluent's director of compliance asked the company's publisher development manager if he had "any thoughts on how we get Nexys to cut this stuff this out" because the claims in a Nexys nutritional supplement ad were "100% false & deceptive" and similar to misrepresentations highlighted in a recent FTC enforcement action. Just over a month later, a Fluent compliance manager brought a similar non-compliant Nexys email to the attention of the publisher development manager, who in turn forwarded it someone on his team with the following instructions: "Get Nexys to cut this if you can...unless you're telling me it's big volume." Between February 2017 and December 2019, Nexys campaigns yielded 14.8 million registrations on jobs and rewards sites, corresponding to approximately \$9.6 million in commissions for Fluent.
- 78. In yet another instance, a Fluent sales manager contacted a publisher about "extremely noncompliant prelanders" that deceptively promoted \$1,000 Walmart gift cards. The sales manager noted that the publisher had already received several warnings, threatened to withhold nearly \$60,000 in revenue generated from the non-compliant pages, but then indicated that the amount was negotiable. The publisher apologized, promised to increase traffic, and asked if the manager could "cover it." In response, the manager suggested he could resolve matters with the compliance team if the publisher committed to averaging \$10,000 in daily revenue.

## B. Defendants Endorse Publishers' Misconduct

79. In many circumstances, Defendants' facilitation of publisher misconduct has extended to outright endorsement of such misconduct.

- 80. For example, in May 2019, Fluent's director of publisher development provided an existing publisher with examples of email ads used by what he described as the company's "top email partner." The examples included misleading claims such "please submit an answer below" to "have this \$1000 CHECK sent to you," and "\$1000.00 has been pre-loaded onto this PAYPAL card, so please act as soon as possible to have it delivered." *See* Compl. Attach. 1, at 6-7.
- 81. In a June 2019 email to one of Defendants' largest publishers, All Inbox, the president of Fluent's performance media group, which oversees the publisher development division, noted that he had received complaints from consumers asking how to schedule their job interview, and in response, inquired how it would impact All Inbox if Defendants required the company to stop "implying or promising" interviews. All Inbox's vice president, Jason Jacobs, stated that this would "have a huge impact" because the claims are used in over 90% of All Inbox's ads and they "easily perform the best." In an exchange later that month, Jacobs confirmed that All Inbox had not "made any changes to the content." The Fluent executive raised no objections but instead suggested that Jacobs promote Amazon jobs because "that one would kill for you guys." Between February 2017 and December 2019, All Inbox generated 48.5 million clicks to Fluent's jobs sites, resulting in 31.6 million registrations and \$12.7 million in revenue for Defendants.
- 82. Similarly, in October 2019, the same Fluent executive intervened in compliance enforcement against the publisher HasTraffic. Although Defendants had not authorized this publisher to promote their websites using text messages, Fluent learned that HasTraffic was doing so and that its messages deceptively promised consumers that they had won a \$1,000 Walmart gift card. After Fluent's director of compliance instructed the publisher development group that "HasTraffic should absolutely not be sending [text messages]," the executive replied that this

"opinion" was "noted" and proceeded to edit the deceptive messages to make them more "tame."

The messages approved by the executive, along with underlined edits, include the following:

- a. Hey (name)! Join us for today's \$1000 gift card <u>promotion</u>! Offer expires at (XX AM or PM) -> (link)
- b. Hello (name), what if we told you that you're just 1 click away from \$1000 Walmart Gift card promo? (link) Get yours now!
- c. Congratulations (name), you are among a group of lucky users selected for this promotion! (link) spin the wheel and follow steps to claim \$1000 gift card now!
- d. Wonderful Walmart Wednesday, (name)! Your email has been selected for today's \$1000 gift card promotion! (link) Click now and follow instructions!
- 83. When one of the executive's subordinates suggested the claim that consumers are just "1 click away" from the \$1,000 promo seemed "a bit aggressive," the executive disagreed, explaining: "You are one click away from the promo (which I stressed). Not getting a gift card. That's a fact that can't be disputed."

# III. <u>Defendants' Publishers Engage in Illegal Spamming</u>

- 84. As Defendants are aware, their publishers have sent emails promoting Defendants' sites to consumers more than ten days after those consumers submitted requests not to receive such emails. Defendants have received numerous complaints from consumers about such conduct.
- 85. Fluent has used a service called Optizmo to collect consumer requests to opt out from emails promoting Fluent's sites and detect publisher failures to honor such requests. These opt-out requests are compiled into a "suppression list." Fluent's terms and conditions require each publisher to "update its suppression list at least 10 days prior to sending any emails on Fluent's behalf." Fluent receives an email alert any time a publisher has failed to download Fluent's updated suppression list for ten days or if a user complains about receiving an email promoting Fluent's

sites more ten days after submitting an unsubscribe request. From February 2017 to March 2020, Defendants received hundreds of Optizmo emails, many of which contained multiple consumer complaints and alerts that publishers had failed to download the suppression list.

86. Despite knowing of publishers' failure to honor these requests, Defendants have failed to discipline or terminate publishers engaged in this misconduct. Instead, Defendants have continued to authorize and pay them to send commercial emails on their behalf promoting Fluent's sites.

## IV. Defendants' False and Misleading Ads

87. In numerous instances, Defendants have also promoted their lead generation websites using their own ads. Defendants have circulated their ads through the internet, including through search engine and banner ads and through social media services such as Facebook, Instagram, Messenger, Snapchat, and TikTok. Defendants have also circulated ads through radio and television commercials.

#### A. Defendants' Deceptive Reward Ads

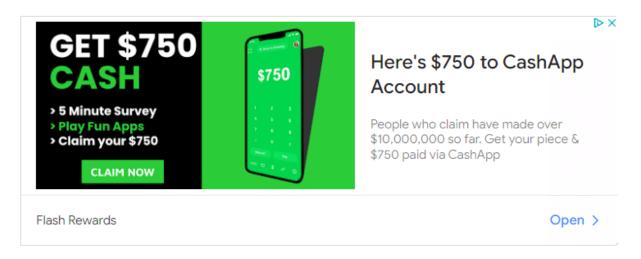
- 88. In numerous instances, Defendants have disseminated ads claiming that consumers can obtain rewards for "free." Other ads claim that the rewards are essentially "fast" or "easy" to obtain. *See, e.g.*, Compl. Attach. 1, at 8-10.
- 89. For example, starting in May 2022, Defendants began running multiple versions of an ad on Facebook and Instagram consisting of a 34-second video accompanied by the caption "Add \$750 To Your Cash App Account!" The video shows a smartphone screen that appears to be running Cash App. A woman's voice can be heard making the following statement:

So keep in mind that this method is 100% for free. Right, so that's crazy -100% for free. So once it's done as you guys can see you guys have to wait until the end and follow all the rules it asks you to do and once you have, go ahead open up your Cash App. Just maybe wait a few seconds. Once you open up your Cash App you guys are going to see instant

money being added to your Cash App as we speak. It's super easy guys. You see it before your eyes and guess what? It didn't charge me anything, it was 100% for free.

While the narrator speaks, the balance of the depicted Cash App account rises from \$0 to over \$300 by the end of the video.

90. In other ads, Defendants have touted the speed with which consumers can obtain rewards. For example, in the following ad, Defendants have claimed that consumers can obtain \$750 by merely completing a "5 Minute Survey" and "play[ing] fun apps."



- 91. Similarly, Defendants have claimed that consumers can obtain a \$750 Cash App reward "This Week" or "Today" or "Qualify in 30 Minutes" for a \$75 Target gift card. Other promoting an \$800 shopping spree at the online clothing retailer Shein claim that "program requirements" can be completed in a single day.
- 92. As set forth below, these reward ads are false and misleading. Defendants' rewards are neither free nor capable of being obtained by simply completing a survey. Consumers must pay money to obtain these rewards. Also, upon information and belief, there are no circumstances in which consumers can obtain a reward from Defendants in 30 minutes, a day, or even in a week.
- 93. In numerous instances, Defendants' ads highlight the amount of money purportedly "given out" to consumers in connection with its reward offers. For example, the ad above claims

that "people who claim [a reward] have made over \$10,000,000 so far." These ads do not disclose the miniscule percentage of consumers who succeed in obtaining a reward.

# B. <u>Defendants' Deceptive Job Ads</u>

- 94. In numerous instances, Defendants' have disseminated ads claiming that consumers can obtain high paying jobs with attractive benefits, some of which target senior citizens in particular.
- 95. For example, as reflected in the following image, Defendants circulated an ad on social media claiming that companies are "now hiring: seniors," offering "work from home jobs" paying up to \$31 per hour.



- 96. In other ads, Defendants have claimed consumers can obtain high paying jobs with attractive benefits working as a "product tester," "video game streamer" or Disney cast member." For example, Defendants have run ads on social media platforms claiming consumers can earn up to \$41 per hour along with an array of perks working from home for Disney. Compl. Attach. 1, at 11.
- 97. As set forth below, the jobs promoted in Defendants' ads often do not exist. Instead, when consumers click on the links in the ads, they are taken to a Fluent job site where they are gradually induced to disclose more and more personal information as they continue to pursue a job opportunity that never materializes.

# V. Defendants' False and Misleading Lead Generation Websites

- 98. Deceived by the misleading ads circulated by Defendants and their publishers, many consumers have clicked on hyperlinks within the ads and have been directed to Defendants' lead generation websites. On these websites, consumers have been misled into divulging personal information that, unbeknownst to many consumers, Defendants have aggregated and sold to advertisers, call centers, and data brokers.
- 99. Defendants' lead generation websites have employed a variety of deceptive design techniques, commonly known as "dark patterns," to manipulate consumers and undermine their ability to make informed choices about their personal information. Some of these tactics include:
- a. Concealing key disclosures by presenting them in small, washed-out text that is barely legible to the naked eye, especially on a mobile device, or hiding these disclosures behind a hyperlink;
- b. Distracting consumers with large, brightly colored gift cards, congratulatory messages, and other embellishments unrelated to the acquisition of consent to receive

telemarketing, email, and text message solicitations that draw attention away from, and often controvert, fine print disclosures;

- c. Obtaining permission to sell consumers' personal information through subterfuge, including disguising telemarketing consent requests as "surveys," and misleading consumers into believing that they are merely "confirming" the "accuracy" of their information or that it is needed to complete a job application; and
- d. Misleading consumers into believing that they are required to provide consent to receive robocalls through the use of hidden or non-existent methods of exiting the consent and information collection process.
- 100. Defendants have also tricked consumers into clicking a single, deceptively labeled checkbox, which they have treated as blanket consent for receiving telemarketing solicitations from dozens or even hundreds of third parties. The purported agreements generated from these "consent farm" websites are a crude attempt to circumvent the TSR's requirement that, to initiate a robocalls, the *specific* seller obtain consent *directly from* a consumer, and only after providing *clear and conspicuous* disclosure.
- 101. Defendants' attitude toward the consumers whose information they monetize is reflected in testimony given by Fluent's general counsel in connection with a private class action lawsuit brought against Defendants. When asked if Defendants had conducted any testing to determine whether consumers are aware of what they are agreeing to, he responded:

Can you explain to me what element of the TCPA requires that consumers be aware that they've given consent. They're supposed to give their prior express written consent...Whether the consumer is actually aware that they're actually doing something or not, I can only assume that most consumers, if they're not aware that their [sic] doing something, they should be aware that they're doing something.

28

#### A. Defendants' Deceptive Reward Websites

102. Defendants have maintained thousands of reward sites used in connection with their

lead generation business. These sites consist of two sections: the consent funnel and the deal wall.

- 103. The consent funnel has included a series of linked surveys and forms that prompt consumers to answer questions, gradually submit more and more personal information, and purportedly consent to the sharing of this information with third parties. Defendants have induced consumers to progress through these pages by falsely suggesting that consumers are merely "confirming" the accuracy of their personal data as part of a required "registration" process while concealing disclosures explaining that this data will be sold to third party marketers.
- 104. After navigating the consent funnel, consumers reach the deal wall, which consists of various third-party offers that consumers must participate in to qualify for a promised reward.

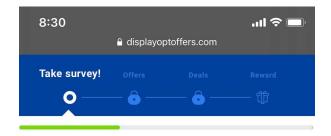
# i. The Consent Funnel

- 105. The first page consumers encounter on one of Fluent's reward sites prominently features an image of a gift card above a question such as, "Do you like to shop online?" along with two large, brightly colored buttons "YES" and "NO." Clicking either button advances to the next screen. The page also contains links to program requirements, FAQs, terms and conditions, and a privacy policy. However, on a mobile device, which accounts for 80-85% of consumer interactions with Fluent websites, these links are not visible unless one scrolls to the bottom of the page.
- 106. After answering additional questions, consumers eventually reach a screen in which they are prompted to "confirm" their email address then click a large blue "Continue" button. But, in small gray text on the page, consumers are informed that by clicking "continue," they agree to the "Privacy Policy." *See* Compl. Attach. 1, at 12. That policy, which is hyperlinked in the inconspicuous text, purportedly authorizes Defendants to sell consumer information to unidentified "Marketing Partners" and "other third parties."
- 107. Consumers who submit an email address and click the "Continue" button next see a screen prominently featuring an image of a gift card, where they are informed that "registration"

is "required" and are prompted to "fill out the basics." The information solicited by Defendants is far from "basic." It includes consumers' name, shipping address, date of birth, gender, and mobile phone number. Finally, there is another large blue "Continue" button. *See* Compl. Attach. 1, at 13-14.

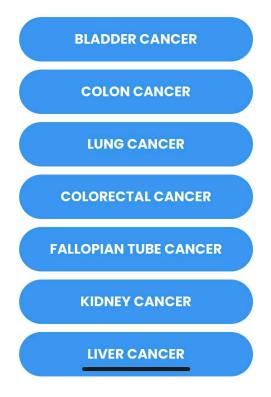
- 108. Again, small gray text at the bottom of this page states that, by hitting the "Continue" button, consumers agree to the same hyperlinked privacy policy, which authorizes Defendants to sell consumer information. Consumers cannot advance to the next screen to purportedly obtain the promised reward without providing the requested information and agreeing to Defendants' privacy policy.
- 109. After entering their information, consumers are shown a screen stating: "Now just take our **quick survey** and follow instructions to get your [reward]! It's that easy!" Consumers are then presented with a series of survey questions soliciting a range of private information, including information about consumers' medical and financial condition, employment status, health history, and insurance needs.
- 110. The "quick" survey can include dozens of questions. Consumers are shown the question and several potential answers in the form of large blue buttons that appear as if they must be clicked to advance onward. Defendants used these questions as a ruse to obtain consumers' purported consent to receive telemarketing and text message solicitations, including robocalls.
- 111. In the example that follows, consumers are asked whether they or a family member has a history of cancer. Placed above several large blue options detailing various forms of cancer is a small fine print disclosure. According to that disclosure, *any* answer to this question allows both "The Ferraro Law Firm," as well as unidentified "third parties," to contact consumers on their

mobile phones via "recurring autodialers" about consumers' use of the drug Zantac, even if their numbers are listed on the Registry or similar state registries.



# Do you or a family member have a history of cancer?

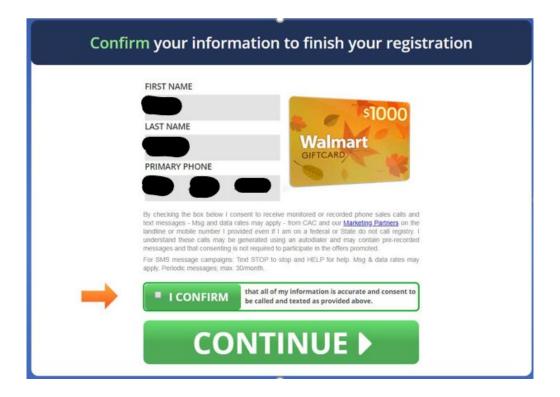
By submitting your information, you agree to our Terms and Conditions and Privacy Policy and consent and request to be contacted by The Ferraro Law Firm and third parties regarding your use of Zantac by using automated technology including recurring auto-dialers even if the phone number you submitted is a mobile number or is currently listed on any state, federal, or corporate "Do Not Call" lists.



112. Instead of clearly and conspicuously informing consumers that their answer could trigger the receipt of telemarketing and text message solicitations, including from unidentified "third parties," Defendants have misled and distracted consumers with personal questions. Indeed,

at least one former Fluent client, upon discovering that it was buying leads generated from such subterfuge, described the practice as "misleading" and stopped doing business with Fluent after the company refused to make requested modifications.

- 113. After responding to various survey questions, consumers eventually reach a screen that purports to obtain their express written consent to receive telemarketing and text message solicitations, including robocalls. Defendants have not sought this consent on their own behalf, but for several third-party sellers and telemarketers pitching a variety of unrelated products and services. In numerous instances, Defendants have purported to obtain consumers' consent to receive robocalls on behalf of dozens or even hundreds of entities.
- 114. From approximately 2019 to 2021, these consent screens prominently featured an image of a gift card. The stated purpose of this page was to "confirm" consumers' "information" to finish their "registration." Immediately below this message were fields provided for consumers' first and last name as well as their phone number. To reinforce the deception that consumers were merely "confirming" information for registration purposes, these fields were typically prepopulated with information provided by consumers on earlier screens. As shown in the following example, occupying the bottom of the screen were two large green buttons labeled "I CONFIRM" and "Continue," with the former accompanied by a checkbox.



See also Compl. Attach. 1, at 15.

115. In contrast to the prominent, colorful design aspects of these screens that draw consumers' attention to confirming information for "registration" purposes, Defendants minimized the consent disclosure in a block of small, gray text inconspicuously set against a white, non-contrasting background. This text stated that by checking the "I confirm" box, consumers consented to receive "monitored or recorded phone sales calls and text messages," including calls that "may contain pre-recorded messages," from unidentified "marketing partners." The text next to the "I confirm" box then confusingly stated that by checking the box, consumers were both confirming the accuracy of their registration information *and* also consenting "to be called and texted as provided above." The inconspicuous text above and in the "I confirm" box did not cure the deceptive net impression that the purpose of these screens was to "confirm" consumers' personal information as a part of the rewards registration process, as opposed to obtain consumers'

consent to sell their personal information to third parties who would then call and text them about topics unrelated to the gift card.

- 116. Moreover, in numerous instances, Defendants have also used images and design elements such as a large arrow pointing to the checkbox to convey that consumers must confirm their information in order to "continue" to the next page, as they try to complete the "registration" to obtain the promised gift card.
- 117. According to the inconspicuous block of text rendered in small, gray font set against a white background, consumers who clicked the checkbox on these pages and proceeded to the next screen agreed to receive telemarketing and text message solicitations, including robocalls, from Defendants' "marketing partners." The identities of these third parties, which are integral to the consent sought from consumers as well as inseparable from it, have been concealed on a separate page that could only be accessed by clicking a hyperlink within the small disclosure text.
- 118. When clicked, the "marketing partners" hyperlink has not identified the specific party or parties from whom consumers were purportedly consenting to receive telemarketing calls and texts. Instead, it opened a pop-up window displaying an alphabetic list presented in small, gray text against a white background that could be hundreds of entries in length. A message at the top of the screen explained that the list consisted of Defendants' "call center/marketing partners" and that a "select group...may contact you by telephone and/or SMS text messaging." Consumers therefore had no way of determining the specific entities from whom they were consenting to receive calls or texts.
- 119. Particularly on a mobile device, Defendants' "marketing partners" pop-up list has often occupied multiple screens and cannot be viewed in its entirety without scrolling extensively. The following is a partial example of such a list:

M - Magazine Direct, Marchex, MDFHoldings, LLC MedHelp, Media Mix365 LLC, Medical Alert Center, Medical Care Alert, MedSavings, Medx Publishing, Inc. MobileDeals MobileSavings, Mutual of Omaha Insurance Company, My Job List, Inc.

N - NAMC, National Disability, National Magazine Exchange, National Med Group, NationalHomeProject.com, Nationwide Vehicle Assurance, NOC Solutions, North American Power & Gas, LLC, NutrisystemAffiliate. NutrisystemPartner, NutrisystemPub O - Oasis Financial, Olympus Medical Group, Omni Research, OpenJar, Orthotic Care, Outside the Box Ovation Credit Repair P - PA Healthcare Pharmaceutical, PainMSG, PALMco. LLC, Palo Media Group, Patriot Trust Lending, Pet First Healthcare, PetHelp, Pharmacy Group, PhoneDeals, PickMyDegree, PillPack, PillPack, Inc., Power Source Marketing LLC, Precision Marketing, LLC, Preferred Pharmacy, Prize MSG, PrizeCentr, Protect My Car Q - Q3M Insurance Solution, Quintessa Marketing R - RateMarketplace, Reality Debt Solutions, Recruit Military, ReliantOne, Renttoownenterprise.com, Research Rewards, Residents Energy, LLC, Rewards4U RewardsMSG, Royal Sea Cruises, Inc., RXAssistProgram S - SACT, SACT MSG, SafeStreets, SafetyNow, Satellite Country, Save Better, SaveAuto, SaveCash, SaveHelp, SaveMobile, SaveMore, SaveMSG, SaveNOW. Schools.com, Senior Care Authority, Septic Maxx, LLC, Septic Savior, Simple Health, Simple Health Plans Inc. Simple Insurance Leads, SizzlingCreditCards, Solid Quote LLC, Split Rock Development, LLC, SpotDeals, Sprint, Start A Career Today, StartaCareerToday.com, Student Loan Forgive, Subcription Ink, Co., Sunrise Communications AG SurveyRedemption, SurveyRedemption.com SurveyRedemption.com/Research Rewards, Sweeps Entry Center, SweepsCraze.com, Sweepstakes Entry Center, SweepstakesADay, SweepstakesEntryCenter, Synergy Attorney Services, LLC T - Talking Customers, Teletransform, Inc., The Bill Wizard, The Credit Pros. The Degree Source, The Ridge Tahoe The Wellness Center, The-Solar-Project.com, Time 2 Read, Time2Read, T-Mobile International AG, Town Square

- 120. Many of Defendants' "marketing partners" are acronyms and generic DBAs, such as "CAC," "RMC," NAMC," "EarnMore," "Prize Centr," and "SaveToday," that provide consumers with little or no information about the products and services marketed by these entities.
- 121. Other names on Defendants' list suggest consumers will be solicited regarding an array of unrelated products and services, including everything from health insurance, solar power, pharmaceuticals, magazine subscriptions, political advocacy, home improvement, cruises and travel, sweepstakes and promotions, credit repair, pain cream, employment and educational opportunities, legal services, and more. By checking a box confirming that their information is accurate for the purpose of completing their gift card registration, consumers do not expect that they will then receive such a broad array of unwanted solicitations. Such bait-and-switch tactics are inherently deceptive and are not a reliable indicator of consent.

- 122. In fact, as illustrated by Defendants' experience with one client, these policies render the concept of express written consent utterly meaningless. With Defendants' knowledge, a client used the DBA "Support First" to robocall consumers for the purpose of selling "free" cruises, home warranties, and hearing aids. Under a different DBA, "Career Advisor," the same client pitched "walk-in tubs," home warranties, hearing aids, and prescription delivery via robocalls. A Fluent sales executive initially raised the concern that "Career Advisor" and another DBA used by the client were not disclosed in Fluent's marketing partners list but then immediately dismissed this concern by rationalizing that Defendants "can't expect [the client] to change their business model overnight." Other clients use a single DBA in connection with as many as ten separate call centers or campaigns.
- 123. After learning about the FTC's investigation, Defendants revised the appearance of their consent screen. However, Defendants have continued to conceal the identities of their "marketing partners" behind a hyperlink, use a "consent" checkbox that also confusingly asks consumers to confirm the accuracy of their information, and do not offer a clear option for bypassing this screen.
- 124. As a result of these and other deceptive design techniques, including the absence of any prominent method for bypassing these pages without providing consent, consumers typically believe that they are merely "confirming" the accuracy of their personal information in order to receive the promised reward, not consenting to the sale of their information to an array of unidentified third-party marketers.
- 125. Amazingly, the dozens or hundreds of names on Defendants' concealed marketing partners list does not represent the full spectrum of entities from whom consumers are allegedly "consenting" to receive solicitations. This is because Defendants have allowed clients to engage

in "cross-selling" and "down-selling," where a client transfers consumer calls to different advertisers selling other products and services. Defendants have not identified these additional advertisers in their already grossly deficient consent disclosures.

### ii. The Deal Wall

- 126. After being lured through the consent funnel, consumers have reached Fluent's "deal wall," where they have been presented with a variety of third-party offers or "deals" that they must complete to qualify for their chosen reward. These deals are grouped into five different "levels," and reward qualification is based on a convoluted set of rules requiring consumers to complete a specific number of deals at different levels depending on the value of their reward. For example, consumers who have selected a \$1,000 reward must complete a total of 25 deals consisting of one level 1, one level 2, three level 3, five level 4, and fifteen level 5 deals. By contrast, a \$100 reward requires the completion of one level 1, one level 2, and three level 3 deals.
- 127. Many deals require consumers to sign up for trial offers that automatically bill them for goods and services each month until they are canceled. Defendants have misleadingly failed to disclose on their deal wall the costs that consumers will incur after these trial subscriptions ends. For example, one such deal involves a 7-day trial subscription to BeenVerified, a background check service, "for just \$1." See Compl. Attach. 1, at 16. However, Defendants' deal wall has not disclosed that consumers would be automatically billed \$26.89 per month when the 7-day trial period expires.
- 128. Another tactic Defendants have employed to obfuscate costs includes preventing consumers from viewing deals available at higher levels until they have completed the deal requirement at their existing level. Thus, a consumer attempting to earn a \$1,000 reward, which requires the completion of fifteen level 5 deals, cannot view deals available at level 5 until completing the ten deals that must first be satisfied on levels 1 through 4,

- 129. After completing the number of deals required for their reward, consumers must initiate the claim process, which often involves: (a) the submission of a notarized claim form, government identification, and proof of current home mailing address; (b) the submission of a "Manual Credit Packet" for deals not automatically credited to a consumer's account; and (c) days or weeks of correspondence with Defendants' customer service department.
- 130. Defendants have not clearly and conspicuously disclosed at any juncture in the registration or rewards qualification process the full extent of the costs and obligations consumers must incur to obtain their promised reward. To the contrary, in many instances, Defendants have provided consumers with incorrect or conflicting information. For example, consumers who click certain misleading reward ads circulated by Defendants are directed to a Fluent pre-lander site falsely stating that only 10 deals are required to qualify for an \$800 reward.
- 131. Based on consumer experiences, the costs and obligations that consumers incur in attempting to complete the required number of deals are substantial. Consumers often report spending weeks and significant sums of money attempting to qualify for a reward only to encounter repeated delays and additional requirements. Many consumers, for example, are informed that if their accounts have not been credited for a deal, they must provide Defendants with proof in the form of URLs, screen shots, receipts, and documentation that is no longer available to them.
- 132. Scores of consumers are unable to timely complete the verification process for myriad other reasons, including Defendants' pervasive failure to respond to customer service inquiries. Thousands of exasperated consumers have filed a complaint with the Defendants themselves, the Better Business Bureau, the FTC, or another third party.

- 133. Defendants' Byzantine qualification requirements and abysmal customer service exhausts consumers and dramatically limits the number of rewards issued. Indeed, the vast majority of consumers obtain nothing from Defendants after disclosing their personal information.
- 134. The ads touting that rewards are "easy" to obtain are flatly contradicted by evidence showing the astonishingly small number of consumers who succeed in receiving a reward—much less than 1%. By definition, the Fluent rewards process cannot be characterized as "easy" if over 99% of consumers who attempt to complete the process ultimately fail.
- 135. From February 2017 through March 2020, only 0.00402% of consumers who registered on a Fluent rewards site succeeded in obtaining the reward that attracted them to these sites in the first place and induced them to compromise their privacy. Put another way, that's 7,527 people out of the 187 million who provided their personal information by registering on one of Fluent's sites. Moreover, just 12.36% of consumers who registered on a rewards site during the same time period completed a single deal, and only 1.44% completed two deals.
- 136. Given the substantial financial and administrative burdens associated with obtaining a reward, the ads touting "fast" rewards are likewise false or misleading, particularly those that promise rewards within 30 minutes to a week. In fact, Defendants' own websites have contradicted their ad claims that consumers can obtain rewards in 30 minutes to a week. According to a section on their website captioned "How fast can I get my Reward," Defendants estimate that completing the deals required to obtain a reward and having those deals validated will take 10 to 14 days. Additional information contained in hyperlinked terms and conditions estimates that the validation process alone can take as long as 10 business days. Consumer correspondence shows a process plagued by delays in which customer service representatives often inform consumers that the wait to receive their reward will "typically" be 30 days.

137. Moreover, the ads claiming that rewards are "free" are false and misleading; depending on the value of the reward, consumers must spend substantial sums of money on the required deals to qualify for a reward.

#### B. Defendants' Deceptive Job Websites

- 138. Defendants' job sites have operated on the same bait-and-switch principles as their reward sites, namely: they have amplified misrepresentations made in ads about the prospect of job interviews and the availability of jobs with specific employers in a consumer's geographic area; and they have gradually induced consumers to submit more and more personal information, purportedly to obtain access to those interviews and jobs.
- 139. For example, in numerous instances, Defendants have claimed they need consumers' contact data "from [their] resume[s]" so that it can "match" consumers with available jobs in their area, "confirm" the accuracy of their contact data, "help" consumers "qualify for more jobs," and complete their "job profile." Defendants have also presented surveys like those described above, which deceptively seek to obtain consumers' consent to receive telemarketing solicitations.
- 140. In reality, this process is an elaborate ruse designed to trick consumers into surrendering their personal information so that Defendants can sell it to third parties, many of whom will use it to pitch products and services unrelated to employment opportunities.
- 141. The following Fluent signup flow from January 2022 represents a typical consumer experience with one of the Fluent job sites:
- a. One of Defendants' publishers sends an email with a subject line "RE: Your upcoming Interview," announcing "UPS is Hiring!" and "Available Positions" include "Package Handler," "Short Haul Driver," "Customer Service," and "Warehouse Asst. Manager." This email contains a hyperlink, which funnels consumers to the landing page of one of Defendants' job sites.

- b. This page features a large image of the letters "UPS" rendered in the company's trademark brown and gold colors, implying an affiliation with UPS. Beneath this image is the heading "UPS Jobs," a text box to enter a zip code, and claims that jobs start at \$15 per hour, applicants are needed, and signing bonuses may be available. *See* Compl. Attach. 1, at 17.
- c. After providing a zip code, consumers advance to another screen, shown below, which prominently displays both the trademarked UPS logo and its slogan, "We [Love] Logistics." Consumers are instructed "enter your name and email to continue." Consumers can only bypass this screen if they see and click the word "skip" rendered in small, barely visible text in the upper right-hand corner of the screen. Disclosures about Defendants' information collection practices are presented in similarly inconspicuous text below the fields for consumers' information.



- d. Further down the same page, beneath a "Submit" button, a statement notes that consumers must consent to the sharing of their personal information with Defendants' "marketing partners" to access job listings. This disclosure is presented in a block of small, gray text; on a mobile device, it is not visible without scrolling to the bottom of the screen. *See* Compl. Attach. 1, at 18.
- e. After submitting a name and email address, consumers advance to a screen, that asks them to "Confirm" their birth date and phone number. This screen includes a small-print disclosure informing consumers that by checking an "I Agree" box and clicking "Submit," they expressly consent to "to be called and/or receive text messages" from Defendants' "marketing partners," and that such calls "may include prerecorded messages." *See* Compl. Attach. 1, at 19.
- f. Like Defendants' reward sites, however, the disclosure on this screen is neither clear nor conspicuous. It is rendered in small, gray text against a non-contrasting white background and is surrounded by more prominent messages in bright colors that both distract from the significance of the disclosure as well as further the deception that consumers must provide their contact information to complete a job application or schedule an interview with UPS. Defendants facilitate this deception through their continued and conspicuous use of the trademarked UPS logo and slogan, their inclusion of "apply" in the website URL, the prominent assurance that consumers are "Almost done!" and the instruction for consumers to "Confirm" their age and phone number to "continue."
- g. Moreover, like Defendants' rewards sites, the term "marketing partners" is a hyperlink, but it is often barely discernable as such. Among other things, Defendants have used the same font style, color, and size as surrounding text with only one, barely perceptible distinction: the term is underlined.

- h. When clicked, the "Marketing Partners" hyperlink generates a pop-up that at one point consisted of a 7-page alphabetized list of the dozens of entities from whom consumers are purportedly consenting to receive telephone calls and text messages.
- i. As with the "Marketing Partner" screen displayed to consumers on Defendants' reward sites, a message at the beginning of this list stipulates that a "select group" of these entities "may" contact consumers "by telephone and/or SMS text messaging." Consumers therefore have no way of determining which entities from this list may purchase their information from Defendants.
- j. Many of Defendants' "marketing partners" have no apparent connection to employment opportunities; instead, they consist of insurance brokers, political organizations, forprofit educational institutions, other lead generators, and sellers of miscellaneous products and services such as home security and pain relief.
- k. The net impression conveyed to a reasonable consumer by this example consumer experience, particularly in light of the initial deceptive email, is that the information is required to apply for a position with UPS and securing an interview for such a position. In fact, other versions of the jobs consent screen are even more deceptive, explicitly representing that consumers are "complet[ing]" an "application," not agreeing to receive robocalls *See* Compl. Attach. 1, at 20.
- 142. The described flow is not an isolated occurrence; the extent to which Defendants' various job sites have confused and deceived consumers is illustrated in scores of complaints and inquires filed with Defendants, including:
- a. "[W]hen I trying to search for jobs on your website, all I get is the run around? I have reenter my name, email, DOB, 4 OR 5 TIMES...Around And around never seeing

an application just answer questions like do I want to go back to school. If that what i was looking for then i would find a website about schools. Your website is a [waste] of my time, Please unsubscribe me and delete my personal information."

- b. "U send an email saying Whole Foods is hiring. Which is the company I've been applying to. Then when I click on your email I'm supposed to enter my information all over and answer many questions selling me insurance or continuing my education! This is bullshit! Delete my info immediately and shame on you! I'm simply trying to get a part time job, that is it!!!"
- c. "I would like to interview for a position with FedEx..the site just rotates me to different pages and nothing to put me in contact with employment..help please"
- 143. As these and other complaints make clear, the misleading design of Defendants' job sites, combined with the deceptive ads that drive traffic to these sites, have induced consumers to mistakenly believe that they are providing their personal information to apply for jobs with specific employers, not so that Defendants can sell consumers' information as leads to third party advertisers.
- 144. In exchange for compromising their privacy, at most, consumers have merely received access to publicly available job listings that they could view for free directly from employers or on conventional job aggregation websites without disclosing personal information that Defendants will sell to third parties. In many other instances, consumers have found themselves either presented with irrelevant listings that do not match their stated geographic location and interests, or they are sent on a seemingly endless loop from one deceptive employment website to another, each of which operates on the same bait-and-switch premise as the Fluent sites. In fact, recently, Defendants' job sites have been prominently featuring a post linking to a Fluent

reward site, characterizing the reward promotion as a "side gig earning opportunity," and promising consumers an opportunity to "[e]arn up to \$1,000 from home."

145. On numerous occasions, current and prospective clients have warned Defendants that consent screens on their job sites are legally deficient, highlighting Defendants' practice of concealing so-called "marketing partners" behind a hyperlink as well as the company's deceptive use of terms—including "apply" and "interview"—designed to falsely and misleadingly suggest that consumers' information will be shared directly with potential employers. In response to these warnings, Defendants have generally refused to make any changes.

#### VI. Defendants Help Their Clients Engage in Abusive Telemarketing Practices

- 146. In numerous instances, Defendants used the personal information gathered from consumers through the means described above to sell leads to third-party sellers and telemarketers. Among other things, Defendants have falsely assured current and prospective clients that consumers provided express written consent under applicable laws, including the TSR, to receive marketing solicitations. In turn, Defendants' clients have used the leads to (1) call numbers listed on the Registry; and (2) initiate outbound telephone calls that deliver a prerecorded message to pitch various products and services to consumers.
- 147. Defendants have known or consciously avoided knowing that their clients call consumers who have not granted these third parties consent to contact them via robocalls or at numbers listed on the Registry. Defendants have also known or consciously avoided knowing that these clients do not have a pre-existing business relationship with the consumers they call.
- 148. Defendants are and have been aware of numerous complaints and legal actions against their lead buyers alleging the buyers (i) made outbound telephone calls that delivered robocalls to induce the sale of goods or services when the persons to whom these telephone calls

were made had not expressly agreed, in writing, to authorize the seller to place prerecorded calls to such persons, and (ii) made improper calls to numbers on the Registry.

- 149. Defendants' knowledge of their clients' abusive telemarketing practices is based on alerts regularly generated by Defendants' compliance monitoring service, voluminous complaints filed by consumers related to unwanted telemarketing, and text message solicitations distributed by Defendants' clients. Furthermore, some clients have complained to Defendants that their methods of purportedly obtaining consumers' consent did not comply with applicable laws.
- business as Freedom Financial that was named as a defendant in a class-action lawsuit alleging violations of the Telephone Consumer Protection Act. *See Berman v. Freedom Financial Network, LLC*, 18-cv-01060-YGR (N.D. Cal. Feb. 2018). The court found that, from September 2017 to April 2018, consumer information purchased from Fluent had been used to place nearly one million robocalls to approximately 150,00 consumers, a large percentage of whom complained that the calls were made in violation of their prior do-not-call requests.
- 151. Despite numerous red flags related to another client, Defendants continued doing business with this client, which, upon information and belief, used Fluent-supplied leads to make hundreds of millions of robocalls to consumers.

#### VII. Ongoing Conduct

152. Based on the facts and violations of law alleged in this Complaint, Plaintiff and the FTC have reason to believe that Defendants are violating or are about to violate laws enforced by the FTC, because, among other things: Defendants have a long history of continuous conduct of the type described above; Defendants engaged in their unlawful acts and practices knowingly, and continued to employ unlawful practices outlined above after learning of the FTC's investigation of Fluent; Defendants remain in the lead generation business and continue to gather consumer

information using deceptive and unlawful practices; and Defendants maintain the means, ability, and incentive to engage in similar conduct in the future.

### **COUNT I Rewards Misrepresentations in Violation of the FTC Act**

- 153. In numerous instances, in connection with generating leads for sale to third parties, Defendants, directly or through publishers acting on their behalf and for their benefit, have represented, directly or indirectly, expressly or by implication, that:
- a. Consumers have won or been specially selected to receive a promised reward;
- b. Consumers will receive a promised reward in exchange for completing a survey without any other cost or obligation;
- c. Consumers will receive a promised reward in exchange for providing their personal information without any other cost or obligation;
  - d. Consumers must act quickly to claim a promised reward;
- e. Defendants are acting on behalf of, or are affiliated with, well-known brands and retailers such as Walmart, Amazon, Google, or Verizon;
  - f. Consumers can obtain a reward for "free" or without any cost or obligation;
  - g. Consumers can obtain a reward within 30 minutes to a week; and
  - h. The process of obtaining a reward is easy.
- 154. In truth and in fact, in connection with the representations set forth in Paragraph 153:
- a. Consumers have not won or been specially selected to receive a promised reward;

- b. Consumers do not receive a promised reward in exchange for completing a survey without any other cost or obligation;
- c. Consumers do not receive a promised reward in exchange for providing their personal information without any other cost or obligation;
- d. Defendants' rewards are not limited in quantity or available for only a short period of time;
- e. Defendants are not acting on behalf of, or affiliated with, well-known brands and retailers such as Walmart, Amazon, Google, or Verizon;
  - f. Consumers must pay money or incur other obligations to obtain a reward;
- g. Consumers cannot typically obtain a reward within 30 minutes to a week; and
- h. The process of obtaining a reward is not easy such that the overwhelming majority of consumers who attempt to obtain a reward do not succeed in doing so.
- 155. Therefore, Defendants' representations set forth in Paragraph 153 constitute deceptive acts and practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

### <u>COUNT II</u> Deceptive Failure to Disclose Costs, Obligations, and Rate of Obtaining Rewards

- 156. In numerous instances, in connection with the advertising, marketing, and promotion of their reward offers, Defendants have represented, directly or indirectly, expressly or by implication, that consumers can earn promised rewards by submitting information and completing surveys and that Defendants have distributed millions of dollars of rewards.
- 157. In numerous instances in which Defendants have made the representations set forth in Paragraph 156, Defendants have failed to disclose, or disclose adequately, to consumers who attempt to qualify for these rewards that they must meet other requirements, and often incur costs,

to obtain the promised reward and that only a small percentage of consumers who submit information and complete surveys eventually obtain a promised reward.

158. Defendants' failure to disclose, or disclose adequately, the material information described in Paragraph 157, in light of the representation as set forth in Paragraph 156, constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

### **COUNT III Job Misrepresentations in Violation of the FTC Act**

- 159. In numerous instances, in connection with generating leads for sale to third parties, Defendants directly or through publishers acting on their behalf and for their benefit, have represented, directly or indirectly, expressly or by implication, that:
- a. Consumers have been specially selected by a prospective employer or have been scheduled for an interview with a specific employer;
- b. Defendants are acting on behalf of, or are affiliated with, well-known companies such as UPS, FedEx, and Coca-Cola; and
- c. Consumers can apply through Defendants for high-paying jobs with generous benefits.
- 160. In truth and in fact, in numerous instances in which Defendants and their publishers make the representations set forth in Paragraph 159 of this Complaint:
- a. Consumers have not been specially selected by a prospective employer or have not been scheduled for an interview with a specific employer;
- b. Defendants are not acting on behalf of, or affiliated with, well-known companies such as UPS, FedEx, and Coca-Cola; and
- c. Consumers cannot apply through Defendants for high-paying jobs with generous benefits because the jobs advertised by Defendants do not exist.

161. Therefore, Defendants' representations as set forth in Paragraph 159 of this Complaint constitute deceptive acts and practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

## COUNT IV Misrepresentations Regarding Collection of Personal Information in Violation of the FTC Act

- 162. In numerous instances, in connection with generating leads for sale to third parties, Defendants have represented, directly or indirectly, expressly or by implication, that they are collecting consumers' personal information, including their phone numbers, email addresses, and dates of birth, primarily for the purpose of:
- a. Confirming the accuracy of the information and registering consumers to qualify for a reward;
- b. Submitting consumers' application either for a specific job or for job opportunities that match consumers' stated qualifications or locations;
  - c. Registering consumers for an interview with a specific employer; or
  - d. Matching consumers with jobs and employers.
- 163. In truth and in fact, in numerous instances in which Defendants make the representations set forth in Paragraph 162 of this Complaint, Defendants are not collecting consumers' personal information primarily for the purpose of:
- a. Confirming its accuracy or registering consumers to qualify for a reward, but for the purpose of selling this information to third parties as leads;
- b. Submitting job applications on behalf of consumers or assisting consumers in applying for jobs, but for the purpose of selling this information to third parties as leads;
- c. Registering consumers for an interview with a specific employer, but for the purpose of selling this information to third parties as leads; and

- d. Matching consumers with jobs or employers, but for the purpose of selling this information to third parties as leads.
- 164. Therefore, Defendants' representations as set forth in Paragraph 162 of this Complaint constitute deceptive acts and practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

### **COUNT V Assisting and Facilitating Violations of the Telemarketing Sales Rule**

- 165. In connection with the generation and sale of leads to third parties, Defendants provided substantial assistance or support to "seller[s]" and/or "telemarketer[s]" engaged in "telemarketing," as defined by the TSR, 16 C.F.R. § 310.2.
- 166. In numerous instances, in connection with telemarketing, those sellers and/or telemarketers:
- a. Initiated or caused the initiation of outbound telephone calls to telephone numbers on the Registry to induce the purchase of goods or services, in violation of 16 C.F.R. § 310.4(b)(1)(iii)(B); and
- b. Initiated or caused the initiation of outbound telephone calls that delivered prerecorded messages to induce the purchase of goods or services in violation of 16 C.F.R. § 310.4(b)(1)(v).
- 167. At all relevant times, Defendants knew, or consciously avoided knowing, that the sellers or telemarketers to whom Defendants sold leads were making the unlawful calls in violation of the TSR.
- 168. Defendants' substantial assistance and support, as alleged, violates the TSR, 16 C.F.R. § 310.3(b)

### <u>COUNT VI</u> <u>Misleading Header Information in Violation of the CAN-SPAM Act</u>

- 169. Defendants "initiate" the transmission of commercial electronic mail messages by "procuring" other persons to initiate such messages on their behalf. 15 U.S.C. §§ 7702(9), 7702(10).
- 170. Defendants initiate the transmission, to protected computers, of commercial emails that contained, or were accompanied by, header information that was materially false or materially misleading, such as "from" lines that do not accurately identify the person who initiated the message.
- 171. Defendants' acts or practices, as described in Paragraph 169, violate Section 5(a)(1) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(1).

### COUNT VII Misleading Subject Headings in Violation of the CAN-SPAM Act

- 172. Defendants initiate the transmission, to protected computers, of commercial emails that contained subject headings that would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message.
- 173. Defendants' acts or practices, as described in Paragraph 172, violate Section 5(a)(2) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(2).

# COUNT VIII Knowing Promotion Through Misleading Header Information in Violation of the CAN-SPAM Act

- 174. Defendants know, or should know, in the ordinary course of their trade or business, that commercial emails promoting Fluent's websites contain materially false or materially misleading "from" lines that do not accurately identify the person who initiated the message.
  - 175. Defendants receive or expect to receive an economic benefit from such promotion;

- 176. Defendants have not taken reasonable action to prevent the transmission or to detect the transmission and report it to the FTC.
- 177. The acts or practices described in Paragraphs 174-76 violate Section 6 of the CAN-SPAM Act, 15 U.S.C. § 7705(a).

# COUNT IX Transmission of Commercial Emails After Objection in Violation of the CAN-SPAM Act

- 178. Defendants initiate the transmission, to protected computers, of commercial emails promoting Fluent's websites to recipients from whom it received, more than ten business days prior, a request not to receive any such messages.
- 179. Defendants' acts or practices, as described in Paragraph 178, violate Section 5(a)(4) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(4).

### **CONSUMER INJURY**

180. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act, the TSR, and the CAN-SPAM Act. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers and harm the public interest.

### THE COURT'S POWER TO GRANT RELIEF

- 181. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt violations of any provision of law enforced by the FTC, including the Telemarketing Act and the TSR.
- 182. Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), Section 7(c) of the Telemarketing Act, 15 U.S.C. § 6102(c), and Section 3(c) of the CAN-SPAM Act, 15 U.S.C. § 7706(c), as modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461, the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015,

Pub. L. No. 114-74 § 701, 129 Stat. 599 (2015), and Section 1.98(d) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(d), authorizes this Court to award monetary civil penalties for each violation of the TSR or the CAN-SPAM Act committed with actual knowledge or knowledge fairly implied.

183. Section 19(b) of the FTC Act, 15 U.S.C. § 57b(b), Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c), and Section 7(c) of the CAN-SPAM Act, 15 U.S.C. § 7706(c), authorize this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the TSR or CAN-SPAM Act, including rescission or reformation of contracts, refund of money or return of property, payment of damages, and public notification respecting Defendants' violations, or unfair or deceptive acts or practices.

#### PRAYER FOR RELIEF

Wherefore, Plaintiff requests that the Court:

- A. Enter judgment against Defendants and in favor of Plaintiff for each violation alleged in this Complaint;
- B. Enter a permanent injunction to prevent future violations of the FTC Act, the TSR, and the CAN-SPAM Act by Defendants;
- C. Award Plaintiff monetary civil penalties from each Defendant for every violation of the TSR and the CAN-SPAM Act;
  - D. Award monetary and other relief within the Court's power to grant; and
  - E. Award any additional relief as the Court determines to be just and proper.

Dated: July 17, 2023

#### Of Counsel:

PURBA MUKERJEE
JAMES DAVIS
Attorneys
Federal Trade Commission
230 S. Dearborn Street, Suite 3030
Chicago, IL 60604
Tel: (202) 527-8251
pmukerjee@ftc.gov
jdavis@ftc.gov

Respectfully submitted,

#### FOR THE UNITED STATES OF AMERICA:

BRIAN M. BOYNTON Principal Deputy Assistant Attorney General Civil Division

ARUN G. RAO Deputy Assistant Attorney General

AMANDA N. LISKAMM Director Consumer Protection Branch

RACHAEL L. DOUD Assistant Director Consumer Protection Branch

### /s/ Zachary L. Cowan

ZACHARY L. COWAN (NCBN 53432)
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-353-7728
Fax: 202-514-8742

MARKENZY LAPOINTE United States Attorney

Zachary.L.Cowan@usdoj.gov

JAMES A. WEINKLE
Assistant United States Attorney
Florida Bar No. 0710891
Email: James.Weinkle@usdoj.gov
Office of the United States Attorney
Southern District of Florida
Alto Lee Adams Federal Courthouse
101 South U.S. Highway One, Suite 3100
Fort Pierce, FL 34950
Telephone: 772.293.0945 (Direct)